

U.S DEPARTMENT OF COMMERCE
PROCESS GUIDANCE AND MINIMUM IMPLEMENTATION STANDARDS FOR
IT Security Plans of Action and Milestones (POA&Ms) and Performance Metrics

[This supersedes the *Guidance for Developing Plans of Action and Milestones* (v2, August 2003) and incorporates *Guidance for Operating Unit Submissions of Plans of Action and Milestones and Quarterly Performance Metrics* (v4, August 2003).]

What is the purpose of this standard?

The [DOC IT Security Program Policy and Minimum Implementation Standards](#), sections 3.2.1.4 through 3.2.1.7, establish the policy for development and management of plans of action and milestones (POA&Ms) to track corrective actions when external audits or self-assessments reveal deficiencies in a Department of Commerce (DOC) information technology (IT) security program or system security controls. This standard provides process guidance and minimum implementation requirements for completion of POA&Ms by all DOC operating units. In addition, this standard describes the specifications for the consistent and comprehensive completion of required updates of its IT security POA&Ms and establishes reporting schedules and formats for POA&Ms and IT security performance metrics.

Failure to follow the prescribed format as described in this standard will result in POA&Ms returned to the operating unit for re-work, and possibly result in the operating unit missing the due date established by IT security policy.

What is a Plan of Action & Milestones (POA&M)?

The Federal Information Security Management Act [FISMA, public law 107-347, Title III, subsection 3544(b)(6)]. FISMA requires that agencies establish "...a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency." The Office of Management and Budget (OMB) annually issues reporting requirements – most recently in August 2003 in Memorandum 03-19, [Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting](#). M-03-19, Attachment C describes the OMB requirements for preparation of IT security POA&Ms and performance metrics. OMB has established the POA&M and performance metrics formats and this DOC standard conveys the DOC expectations of those requirements to DOC operating units.

What must be included in a POA&M?

POA&Ms must include all IT security program-level and system-level weaknesses identified as:

- All findings from
 - Office of Inspector General (OIG) reports – public (white cover) and restricted/ sensitive (red cover) reports,

- General Accounting Office (GAO) reports – public (blue cover) and limited official use (gray cover) reports, and
- Third-party contractor assessment reports (such as Department Compliance Review reports, or reports of contractors hired by the operating unit to conduct IT security self-assessments or vulnerability assessments);
- Planned system controls identified in updating a general support system or major application security plan (do not need to track control upgrades or enhancements but must track missing controls);
- Corrective actions necessary to achieve full compliance with Departmental policies and standards (including actions specified in approved policy waiver requests);
- Corrective actions necessary to achieve full accreditation of a system, which must be detailed by the Designated Approving Authority in the interim authority to operate memo to the System Owner; and
- NIST Special Publication 800-26, Appendix A, *system* self-assessment checklist **critical elements** that have not reached Level 4, tested¹, and for which the Designated Approving Authority (DAA) has not accepted residual risk in writing. A Level 4 indicates that there are documented policies (Level 1) and procedures for implementing the control (Level 2); that the control has been implemented (Level 3); and that the control has been tested and if found ineffective, remedied (level 4). The weakness should be tracked at the critical element level and not by control objective or technique.
- IT Security Program capability maturity (NIST Special Publication 800-26, Appendix C) below a Level 3², implemented procedures and controls. At level 3, the IT security *program* procedures and controls are implemented in a consistent manner and reinforced through training. While testing the on-going effectiveness is not emphasized in Level 3, some testing is needed when initially implementing controls to ensure they are operating as intended.

Do I list all weaknesses in one POA&M for my operating unit?

How many POA&Ms you will need depends on the nature of the weaknesses. Weaknesses are of two types: program-level and system-level. For the purposes of the POA&M, the *program* is

¹ As defined in NIST Special Publication 800-26, Level 4 for both IT systems and IT security programs reflects that procedures and controls have been tested and reviewed. The NIST guide explains that “testing and reviewing controls are an essential part of securing a system for each specific control,” and that users are to check whether it has been tested and/or reviewed when a significant change occurred. Within Commerce, testing of all management, operational, and technical controls are required for system certification and accreditation. If a system has not achieved a Level 4, the system owner would have difficulty proving the system is sufficiently secure and requesting authorization to operate from the DAA. Commerce IT Security Program Policy and Minimum Implementation Standards, section 3.2, requires that both systems and programs are required to be assessed annually.

² The five levels on the system self-assessment checklist (Appendix A of NIST Special Publication 800-26) are closely tied to the five levels of the IT Security Assessment Framework (Appendix C of NIST Special Publication 800-26). The IT Security program maturity levels have different criteria than the criteria for determining system control maturity.

the IT security program³ for your operating unit, or in the case of the Department, for the Departmentwide program. A *system* is either a general support system or major application. Each program and each system require separate POA&Ms.

- Program-level weaknesses involve development of policies and procedures applicable to the entitywide IT security program, and are identified through external audits/evaluations, DOC compliance reviews, and operating unit self-assessments.
- System-level weaknesses involve a specific general support system or major application only and are identified through evaluations and audits, DOC compliance reviews, certification testing, and operating unit self-assessments (NIST Special Publication 800-26 self-assessment checklist).

What format do I use to complete the POA&M?

Currently, OMB requires POA&Ms to be submitted in Microsoft Excel format. The central Departmental database will be in Microsoft Access; therefore operating units must submit POA&Ms using Microsoft Excel so that the information can be efficiently imported to the database.

Who is responsible for reporting the POA&M and Performance Metrics and what must be reported?

The operating unit IT Security Officer (ITSO), through the operating unit Chief Information Officer (CIO), must submit the following reports in accordance with this standard. As necessary to comply with OMB reporting guidance, the Department IT Security Program Manager will issue updates to this standard to reflect changes in reporting requirements.

1. Monthly [Summary](#) FY 2003 and FY 2004 POA&M Status Updates
 - a. A Microsoft Excel file containing an updated [summary table](#) for the FY 2003 POA&M (see example at [attachment 1](#)).
 - b. A Microsoft Excel file containing an updated summary table for the FY 2004 POA&M (see example at [attachment 1](#)) or if there are no FY 2004 weaknesses, or no changes since the prior report, a narrative statement that no FY 2004 weaknesses have been identified and/or no changes have occurred.
2. Periodic Submission of Full POA&M Reports with [Detailed POA&M Tables](#)
 - a. A Microsoft Excel file containing the updated detailed FY 2003 [POA&M tables](#) of program-level and system-level weaknesses identified in FY 2003 as prepared

³ For the purposes of program self-assessments, Commerce defines a *program* as a high impact program (such as the IT security program for a Commerce operating unit); a program management division dedicated to the security of a major information system (as defined by OMB Circular A-11) or other or logically related group of systems (referred to by the NIST IT Security Assessment Framework as an asset). The asset owner, in partnership with those responsible for administering the information assets (which include IT systems), must determine whether the measurement criteria are being met at each maturity Level.

and submitted to the Department on September 12, 2003, and by the Department to OMB on October 1, 2003. Examples for the preparation of FY 2003 POA&Ms are provided at [attachment 2](#). Submissions in June and September 2004 must include changes to milestones, including delays to milestones (column F) and update of status (column H).

*[NOTE: After the Department's submission of POA&Ms to OMB on October 1st, operating units **MAY NOT CHANGE** information in columns A, B, C, D, E, or G for any POA&M item. All changes for updates due in January, March, June, and September must be provided in columns F and H **ONLY**.]*

- b. A Microsoft Excel file containing [detailed POA&M program-level and system-level tables](#) for new weaknesses identified in FY 2004 (see example at [attachment 2](#)) or if there are no new FY 2004 weaknesses, or no changes since the prior report, a narrative statement that no FY 2004 weaknesses have been identified and/or no changes have occurred.
 - For new weaknesses identified during FY 2004, operating units must complete a POA&M table for new program-level weaknesses and ITSOs must ensure that system owners complete separate POA&Ms for each system with system-level weaknesses (separate tables for individual systems) identified in FY 2004 (see example at [attachment 2](#)).
 - Instructions for the preparation of FY 2004 POA&Ms are the same as for FY 2003. Provide all FY 2004 tables as separate worksheets of one file. The tables must be developed and submitted in Microsoft Excel format (use a separate Excel worksheet for each separate POA&M). No other formats are acceptable at this time. Spell out acronyms on first use for system names, office symbols, and other terms not readily apparent to the outside reviewer. Provide separate files for the FY 2003 weakness and the FY 2004 weakness tables.

[NOTE: Do not combine new weaknesses identified during FY 2004 into the tables or summary for the FY 2003 POA&M.]

3. [Performance Metrics](#)

Operating units must provide a periodic update on their performance against a set of [IT security measures established by OMB](#). Operating units must use Microsoft Excel and complete the table shown at [attachment 3](#).

[What information is required in the POA&M Summary?](#)

The POA&M summary contains the numerical status of all actions (weaknesses) reported to OMB. [Attachment 1](#) provides an example of completed POA&M summary tables. This summary includes a number for

- Total Weaknesses,
- Actions Completed (including testing),
- Actions Ongoing and On Schedule, and

- Actions Delayed (including explanatory note of the new target completion date and a brief description of the cause of the delay). Delays must also be included in the detail POA&M table, under [column F, “changes to milestones.”](#)

[NOTE: The sum of the Actions Completed, Actions Ongoing and On Schedule, and Actions Delayed must equal the Total Weaknesses]

What information do I include in the POA&M?

Provide all tables for each FY as separate worksheets of **one** file. The tables must be developed and submitted in Microsoft Excel format (use a separate Excel worksheet for each separate POA&M table – see separate file for an example POA&M template). No other formats are acceptable at this time. Spell out acronyms on first use for system names, office symbols, and other terms not readily apparent to the outside reviewer. Provide separate files for the FY 2003 weakness and the FY 2004 weakness tables (see [Attachment 2](#)).

[NOTE: Do not combine new weaknesses identified during FY 2004 into the tables or summary for the FY 2003 POA&M.]

- Column A: The first column of each row in the table must include a brief description of the weakness⁴ or area of weakness found. All weaknesses in the entire POA&M must be numbered sequentially starting with 1.
- Column B: Operating unit’s program office or line office responsible for implementing corrective action⁵ – office names or position titles are preferred over people’s names.
- Column C: Estimated resources required to resolve the deficiency (low, moderate, high) or actual amounts if known. If existing resources will be used and no additional funding will be requested, state “none.”
- Column D: Scheduled final completion date for overall completion of all sub-tasks associated with correcting the weakness.
- Column E: Key milestones with interim completion dates that describe all sub-tasks associated with the correcting the weakness. Separate sub-tasks by using bullets or spacing between tasks.
- Column F: Changes to the original milestones. For **delayed** actions, provide the new milestone completion date and provide a brief description of the cause of the delay.
Note: Provide a concise reason for the delay – per direction of the Secretary of

⁴ The Department of Commerce defines a reportable weakness as: all findings from external audits, reviews, or evaluations (e.g. GAO, OIG, or DOC compliance review reports); significant vulnerabilities found in periodic testing or arising from IT security incidents that the system owner or Designated Approving Authority deems necessary to report; and deficiencies found in self-assessments where a critical system element is below a Level 4 or an IT security program is below a Level 3.

⁵ Corrective actions include: all recommendations from external audits, reviews, or evaluations (e.g. GAO, OIG, or DOC compliance review reports); actions to mitigate significant vulnerabilities found in periodic testing that the system owner or Designated Approving Authority deems necessary to report; and actions to correct deficiencies found in self-assessments and bring a critical system element to a Level 4 or higher or a program to a Level 3 or higher.

Commerce in a 2001 memo, adequate resources must be provided for IT security; therefore, lack of resources will not be accepted as a reason for delay. Missed milestones are a serious matter that must be addressed by all parties involved (system owner, IT security officer, chief information officer, and program officials or operating unit heads) to evaluate the cause and formulate immediate action to enable completion of the corrective actions. For actions *completed early*, provide the actual completion date and reasons for early completion so that efficiencies can be shared Department-wide.

- Column G: Reporting source of the weakness (e.g., OIG audit or NIST self-assessment).
- Column H: Status of corrective actions as of the end of the period covered by the report. You must enter either “Complete” or “Ongoing.” No other description of status is acceptable in this column. If complete, you must include the date of completion, **including testing****. Any other explanatory notes must be entered in the changes to milestones column.

****[NOTE: for an item to be properly categorized as “Complete,” the ITSO must have tested the action’s implementation (e.g., re-scan networks to verify that vulnerabilities were fixed, or visually inspect that new documentation exists and is in final, not draft, form).]*

After the Department’s submission of Fiscal Year POA&Ms to OMB in October, operating units **MAY NOT CHANGE** information in columns A, B, C, D, E, or G for any POA&M item. All status notations and changes for updates due in January, March, June, and September must only be provided in columns F and H.

What do “Project ID,” Project Name,” and “Security Costs” mean on the system-level POA&M?

OMB requires that all systems be tied to the budget process, either as part of a major IT investment, or as included in the agency’s overall IT program or infrastructure funding. If the system is part of a major IT investment for which an Exhibit 300 (capital asset plan and justification) was submitted, you must provide the unique project identifier, system name (spell out acronyms), and security costs as identified in the Exhibit 300. If not part of a major IT investment, provide the Exhibit 53 account code, system name (spell out acronyms), and security costs identified in the Exhibit 53. Further information regarding the budget account codes is available in see [OMB Circular A-11](#).

What information is contained in the Performance Metrics?

OMB Memorandum 03-19, [Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting](#), Attachment C, sets forth the performance metrics content.

- Total Number of Systems – number must agree with the number of systems listed in the IT system inventory.
- Number of systems assessed for risk and assigned a level of risk – of the total number of systems, state how many have had a risk assessment within 3 years.

- Number of systems that have an up-to-date IT security plan – of the total number of systems, state how many have a current system security plan.
- Number of systems certified and accredited – of the total number of systems, state how many have a full accreditation. Note: A system with interim authority to operate is not considered accredited.
- Number of systems with security control costs integrated into the life cycle of the system – of the total number of systems, state how many have security funding on the agency Exhibit 53 funding document and/or have an Exhibit 300 major IT investment business case.
- Number of systems for which security controls have been tested and evaluated in the last year – of the total number of systems, state how many have been evaluated against the NIST Special Publication 800-26 system self-assessment checklist in the past year. If the system was certified and accredited within the past year, this also qualifies as testing all system controls.
- Number of systems with a contingency plan – of the total number of systems, state how many have a comprehensive contingency plan that covers a range of interruptions, from minor backup and recovery procedures to major disaster recovery plans.
- Number of systems for which contingency plans have been tested – of the total number of systems, for those that have contingency plans, state how many have been tested (from minor backup and recovery tests to disaster recovery if appropriate).

What is the FY 2004 POA&M and Performance Metrics Reporting Schedule?

Beginning in FY 2004, three types of submissions will be required: full POA&M reports with detailed tables, summary POA&M status updates, and performance metrics. The DOC reporting schedules for each of these submissions are provided in separate tables below, and a consolidated reporting table is also provided at [attachment 4](#).

- **Monthly POA&M Summary Status Updates**

Operating units must submit summary updates of FY 2003 and FY 2004 POA&M status to the DOC IT Security Program Manager via e-mail no later than close of business on the 5th of the month, or first business day after in accordance with the following schedule.

POA&M Summary Status as of:	Date Due to ITSM
May 31, 2004	June 7, 2004
June 30, 2004	July 6, 2004
July 31, 2004	August 5, 2004
August 31, 2004	September 7, 2004
September 30, 2004	October 5, 2004

- **Quarterly Full POA&M Report with Detailed POA&M Tables and Updated Milestones**

For questions, contact the DOC IT Security Program Manager, Nancy DeFrancesco, at (202) 482-3490 or at NDeFrancesco@doc.gov

Operating units must provide an initial submission of the full POA&M report for FY 2003 weaknesses in September 2003 and beginning in January 2004 provide periodic updates of the FY 2003 detailed POA&M tables and new FY 2004 POA&M tables to the DOC IT Security Program Manager via e-mail in accordance with the following schedule.

POA&M Changes to Milestones and Status as of:	Date Due to ITSM
May 31, 2004 (FY 2003 and FY 2004 updates)	June 7, 2004
August 31, 2004 (FY 2003 and FY 2004 updates)	September 7, 2004

- **Quarterly [Performance Metrics](#)**

Operating units must provide an initial submission of the metrics in December 2003 and provide quarterly updates of the metrics to the DOC IT Security Program Manager via e-mail in accordance with the following schedule.

IT Security Performance Measurement as of:	Date Due to ITSM
May 31, 2004	June 7, 2004
August 31, 2004	September 7, 2004

What are some examples for applying this guidance in developing a POA&M?

Example 1: OIG Report OSE-14788.

Report excerpt: **“FINDING**

“IT Service Contracts Frequently Lack Adequate Information Security Provisions

“Our review of contract actions for information technology services revealed that information security provisions were either totally missing or inadequate.....”

“Contract Information Security Requirements and Oversight Should be Expanded

“The most frequently included information security provisions in IT service contracts are for contractor employee background screening, facilities access, and Privacy Act compliance. However, adequate protection of the Department’s sensitive systems and information also requires safeguards associated with the specific network and computing technologies to be used,...”

“Guidance for Contracting Officers is Minimal and Unclear

“The lack of adequate contract requirements for information security is attributable in large measure to the lack of specific federal and agency guidance on this subject....”

“Information Security Training Should Be Included in Career Development Training for Contracting Staff

“Providing guidance to contracting staff will not be enough: they must also receive training to understand how to apply the guidance.....”

“Recommendations

“...should take the necessary actions to ensure that all contracting offices...include adequate security provisions in all IT service contracts...To accomplish this, various bureaus,...will be required to coordinate their efforts and take the following actions:

1. “...develop and disseminate policy for acquisitions of IT systems and services that requires....a. b. c....”
2. “...establish standard contract provisions...”
3. “...instruct all heads of contracting offices to review all current contracts and solicitations for IT services...”
4. “...ensure that contracting officers...have appropriate training...”
5. “...ensure that contracting officers...are made aware of and use NIST Special Publication 800-4...”

See the [Example 1 POA&M table on page 9](#) to see how to address this OIG report in the POA&M.

Example 1: Completed POA&M Table.

Department of Commerce – *Operating Unit Name (OU)*
Program-Level Plan of Actions and Milestones

Column A	Column B	Column C	Column D	Column E	Column F	Column G	Column H
FY2004 Weaknesses	Office/ Organization Responsible	Resource Estimate funded/ unfunded/ reallocation	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	Identify Source	Status
OU 04.1 IT service contracts lack adequate information security provisions	OU CO	None (existing staff level of effort)	12/31/2004	<ol style="list-style-type: none"> 1. Expand contract information security requirements and oversight: 12/31/04 <ol style="list-style-type: none"> a. Develop and disseminate policy: 12/31/04 b. Establish standard contract provisions: 08/15/04 c. Instruct head of contracting offices to review contracts and solicitations: 06/30/04 2. Develop clear guidance for contracting officers – instruct COs to use NIST SP 800-4: 07/31/04 3. Include IT security training in development of contracting staff: 06/30/04 		OIG Report OSE-14788	Ongoing

Example 2: NIST self-assessment questionnaire Risk Management section showing Critical Element 1 at Level 1 and Critical Element 2 at Level 3.

Operating Unit A, System 1

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management <i>OMB Circular A-130, III</i>	X							
Critical Element 1: Is risk periodically assessed?	Yes	No	No	No	No		Included in Handbook for Information Technology	
Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? <i>FISCAM SP-1</i>	Yes	Yes	No	No	No			
Has data sensitivity and integrity of the data been considered? <i>FISCAM SP-1</i>	Yes	Yes	Yes	No	No			
Have threat sources, both natural and manmade, been identified? <i>FISCAM SP-1</i>	Yes	Yes	No	No	No		DOC Physical Security regularly conducts Risk Assessments	
Has a list of all known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed? <i>NIST SP 800-30</i>	Yes	No	No	No	No			
Has a countermeasure analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? <i>NIST SP 800-30</i>	Yes	No	No	No	No		ITSO staff reviews security Plans and counter measures are provided.	
Has a consequence assessment, which estimates the degree of harm or loss that could occur, been conducted? <i>NIST SP 800-30</i>	Yes	No	No	No	No			

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Critical Element 2: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?			X					
Are final risk determinations and related management approvals documented and maintained on file? <i>FISCAM SP-1</i>	Yes	Yes	Yes	No	No			
Has a mission/business impact analysis been conducted? <i>NIST SP 800-30</i>	Yes	Yes	Yes	No	No			
Have additional controls been identified to sufficiently mitigate identified risks? <i>NIST SP 800-30</i>	Yes	Yes	Yes	No	No			

See the [Example 2 POA&M table](#) on page 12 to see how to address this NIST self-assessment in the POA&M.

Example 2: Completed POA&M Table.**Operating Unit Name (OU) System-Level Plan of Actions and Milestones**

Project ID = 001-62-5800-0000-123-45

Project Name = System 1

Security Costs = \$50K

FY2004 Weaknesses	Office/ Organization Responsible	Resource Estimate funded/ unfunded/ reallocation	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	Identify Source	Status and date completed
OU 04.x + 1 Risk not periodically assessed	Line Office A	None (existing staff level of effort)	12/31/2004	1. Develop comprehensive policy: 09/30/04 2. Develop comprehensive procedures: 11/15/04 3. Implement policies and procedures: 12/31/04		NIST self- assessment	Ongoing
OU 04.x+2 Program Officials' understanding of risk has not been tested	OU CIO/ITSO	None (existing staff level of effort)	12/31/2004	1. Inspect documentation of final risk determinations to ensure they contain related management approvals and are maintained on file. 10/31/2003 2. Inspect the mission/business impact analysis that was conducted and evaluate the adequacy. 11/30/2003 3. Evaluate risk assessment and associated documentation and determine whether additional controls been identified to sufficiently mitigate identified risks. 12/31/2003		NIST self- assessment	Completed 12/31/2003

Attachment 1. Examples of completed POA&M Monthly Summary Tables for FY 2003 and FY 2004.

Department of Commerce/*Operating Unit Name*
FY 2003 Plan of Actions and Milestones
Summary Status as of *mm/dd/yyyy*

Total Weaknesses	Actions Completed (including testing)	Actions Ongoing and On Track	Actions Delayed from Original Completion Date
			Weakness Number, Reason for Delay, and Interim Achievements
32	28	3	1
			OU 03.4 <i>Continuity of service</i> On 3/24/03, the CIO conducted a limited off-site test of contingency and disaster recovery plan procedures. In the first half of FY 2004 IT resources will be focused on full testing of the plan. Target completion date 08/31/2004 (original date 04/30/2004)

Department of Commerce/*Operating Unit Name*
FY 2004 Plan of Actions and Milestones
Summary Status as of *mm/dd/yyyy*

Total Weaknesses	Actions Complete (including testing)	Actions Ongoing	Actions Delayed from Original Completion Date	New Weaknesses Identified During This Reporting Period
			----- Weakness Number, Reason for Delay, and Interim Achievements	
12	1	11	0	5

Attachment 2. Standard field values for POA&M program-level and system-level tables.

[Enter full spelling of operating unit name here]

Program-Level Plan of Actions and Milestones

Column A FY 2003 (or FY 2004) Weaknesses	Column B Office/ Organization Responsible	Column C Resource Estimate funded/ unfunded/ reallocation	Column D Scheduled Completion Date	Column E Milestones with Interim Completion Dates	Column F Changes to Milestones	Column G Identify Source	Column H Status
OU FY.1.1 (e.g., OU 03.1.1 if for FY03) Nature of weakness (cannot be changed)	Office (cannot be changed)	Resources (cannot be changed)	Target completion (cannot be changed)	Milestones and interim dates (cannot be changed)	ALL changes to target completion date and milestones. Include reasons for delays.	Source (cannot be changed)	Ongoing or Complete
OU FY.1.2							Ongoing or Complete

[Enter full spelling of operating unit name here]

Program-Level Plan of Actions and Milestones

53/300 Project ID = 000004444555567890

System Name = nnnnnnnnn

Security Costs = \$xx,xxx

FY 2003 Weaknesses	Office/ Organization Responsible	Resource Estimate funded/ unfunded/ reallocation	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	Identify Source	Status
OU FY.2.1							Ongoing or Complete
OU FY.2.2							Ongoing or Complete

Attachment 3. Standard format for the FY 2004 Quarterly Performance Metrics table.

[Note: Performance Metrics for FY 2005 and beyond will be updated annually by the IT Security Program Manager based on OMB guidance.]

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level of risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%

Attachment 4. Table of Consolidated POA&M and Performance Metrics Reporting Dates for FY 2004 (reporting periods ending May 31 through September 30, 2004)

[Note: Reporting dates for FY 2005 and beyond will be updated annually by the IT Security Program Manager based on OMB guidance.]

Reporting Item	“As of” Date	Date Due to ITSM
Detailed POA&M Tables POA&M Summary Status Performance Metrics	May 31, 2004	June 7, 2004
POA&M Summary Status	June 30, 2004	July 6, 2004
POA&M Summary Status	July 31, 2004	August 5, 2004
Detailed POA&M Tables POA&M Summary Status Performance Metrics	August 31, 2004	September 7, 2004
POA&M Summary Status	September 30, 2004	October 5, 2004

Addendum to
U.S DEPARTMENT OF COMMERCE
PROCESS GUIDANCE AND MINIMUM IMPLEMENTATION STANDARDS FOR
IT Security Plans of Action and Milestones (POA&Ms) and Performance Metrics
(issued by DOC CIO July 28, 2004)

Attachment 4

Table of Consolidated POA&M and Performance Metrics Reporting Dates for FY 2005

Reporting Item	“As of” Date	Date Due to ITSPM
POA&M Summary Status	October 31, 2004	November 5, 2004
Detailed POA&M Tables POA&M Summary Status Performance Metrics	November 30, 2004	December 6, 2004
POA&M Summary Status	December 31, 2004	January 5, 2005
POA&M Summary Status	January 31, 2005	February 7, 2005
Detailed POA&M Tables POA&M Summary Status Performance Metrics	February 28, 2005	March 7, 2005
POA&M Summary Status	March 31, 2005	April 5, 2005
POA&M Summary Status	April 30, 2005	May 5, 2005
Detailed POA&M Tables POA&M Summary Status Performance Metrics	May 31, 2005	June 6, 2005
POA&M Summary Status	June 30, 2005	July 6, 2005
POA&M Summary Status	July 31, 2005	August 5, 2005
Detailed POA&M Tables POA&M Summary Status Performance Metrics	August 31, 2005	September 6, 2005
POA&M Summary Status	September 30, 2005	October 5, 2005